Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2007 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2007

Expanding Views of Technology Acceptance: Seeking Factors Explaining Security Control Adoption

Tim Chenoweth
Boise State University

Robert Minch
Boise State University

Sharon Tabor
Boise State University

Expanding Views of Technology Acceptance: Seeking Factors Explaining Security Control Adoption

Tim Chenoweth
Boise State University
timchenoweth@boisestate.edu

Robert Minch
Boise State University
rminch@boisestate.edu

Sharon Tabor
Boise State University
stabor@boisestate.edu

Abstract

This research in progress essay reviews the existing technology acceptance literature to evaluate its ability to predict the adoption of network security controls. We suggest that an expanded view of current technology acceptance theory may be required to adequately address the complex variables that influence the acceptance of security controls. An important differentiator is that while traditional technology adoption models address potential gains in a positive sense, security control adoption results in the avoidance of a potential harm. This leads to consideration of the security IT artifact using a Herzberg-like two-factor model and the investigation of models outside traditional IT research, such as Protection Motivation Theory. These models offer potentially valuable alternatives by recognizing the importance of factors such as perceived vulnerability and perceived threat severity that are not considered in current technology acceptance literature.

Keywords: IT artifact, security control adoption, threat mitigation, TAM, UTAUT, PMT

Introduction

A large body of work evolving over more than thirty years has examined the concept of technology acceptance. Research from social psychology has been particularly important in helping us understand user motivation and behavior. Both the Theory of Reasoned Action, TRA, (Fishbein and Ajzen, 1975) and the Theory of Planned Behavior, TPB, (Ajzen, 1991) have been used extensively in models attempting to predict behavior. TRA suggests that *intention*, the stage before behavior, is developed from information or beliefs that a specific outcome is likely to result. TPB adds the idea that *perceived behavioral control* also affects intentions and subjective norms. Control assumes the user has the necessary resources and opportunities to perform the desired behavior.

Building upon earlier technology acceptance work, Davis (1989) validated the constructs of *perceived usefulness* (the extent to which people believe technology will help them perform their job), and *perceived ease of use* (how difficult the system is to use) as key determinants of *user acceptance*. This resulted in the widely-used technology acceptance model (TAM) shown in figure 1.

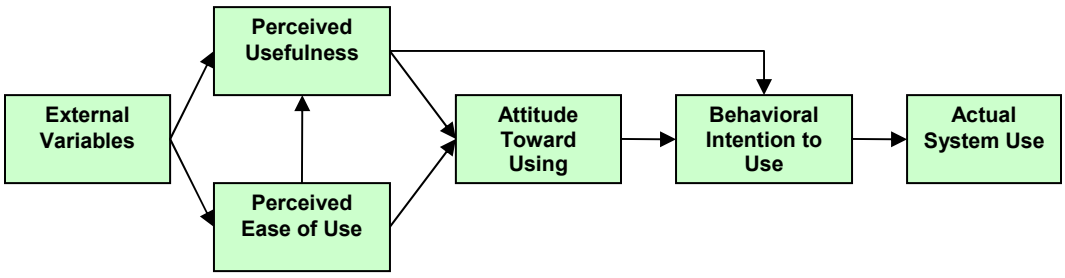

Figure 1. Technology Acceptance Model (Davis, Bagozzi, Warshaw, 1989)

Although various other extensions to the original TAM exist, the *Unified Theory of Acceptance and Use of Technology* (UTAUT) shown in figure 2 represents the most significant modification in recent years. Venkatesh, et al. (2003) examined

and tested eight prominent theories or models (TRA, TAM, Motivational Model, TPB, Combined TAM-TPB, Model of PC Utilization, Innovation Diffusion Theory, and Social Cognitive Theory) to validate the most significant elements and interactions of each, and eliminate duplications among variables. The resulting UTAUT model includes four core determinants of user intentions leading to use, and four moderators of relationships between them, representing the first model that attempts to further define external influences. Moderating variables of *gender*, *age, experience*, and *voluntariness of use*, are included to determine their impact on expectations and outside influences.

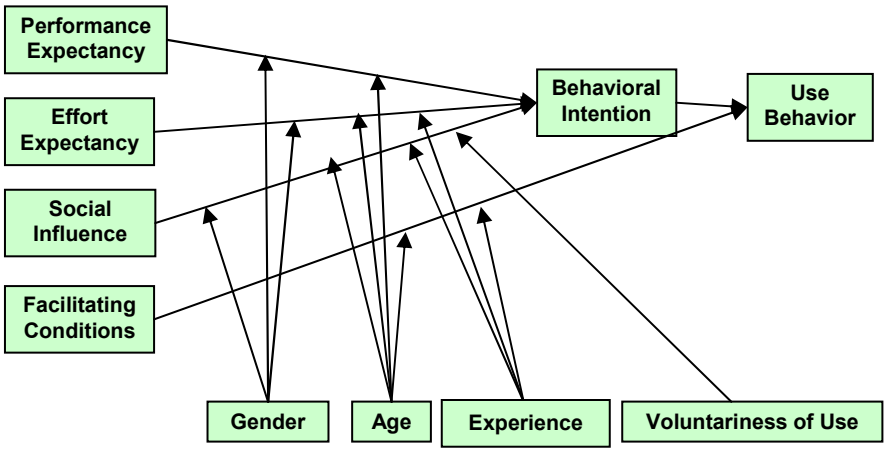

Figure 2. Unified Theory of Acceptance and Use of Technology (Venkatesh, et al., 2003)

While the previously mentioned theories have been applied to many different types of IT systems, one notable exception is the area of network based security controls (e.g. firewalls, virus protection software, etc.). The issue of motivating individual users to implement security controls is becoming increasingly important, in part because of the growing popularity of wireless networks, and in particular free and fee-based public access points, or "hotspots." Recent surveys show that approximately 60% of all wireless networks use no form of encryption (Panda 2006), and technical safeguards are so weak that "For all intents and purposes, security at a hotspot is unachievable, given the current state of the technology" (Potter 2006, p. 52). This means users must be aware of the threat and take action to provide their own system security. Informed network users who are willing and able to comply with security guidelines, including those related to system security on their individual devices, are essential to security for larger organizational networks (NIST 2002). To date, the technology acceptance research community seems to have ignored this important area.

The remainder of this critical essay will look at alternative theories and attempt to identify important commonalities and differences. We first consider the issue of the IT artifact, and discuss how differences between artifacts may influence the determinants of technology adoption. We specifically examine UTAUT and attempt to assess its applicability for explaining security control adoption. We then discuss Protection Motivation Theory (PMT), taken from the protection behavior literature, as an example of a theory that may provide important insights into the adoption of security controls that are not provided by UTAUT. Following this, a comparison of UTAUT and PMT will identify and discuss important differences between UTAUT and PMT, within the context of security control adoption. Throughout the essay we identify important areas where addition empirical research is needed.

New Perspectives for a Security Control Focus

Orlikowski and Iacono (2001) lament the lack of IT research attention paid to the IT artifact, noting that "The IT artifact itself tends to disappear from view, be taken for granted, or is presumed to be unproblematic once it is built and installed" (p. 121). In a taxonomy of IT views taken by researchers publishing in the journal *Information Systems Research* over a ten-year period, the authors identified broad categories looking at IT from five views: "Tool," "Proxy," "Ensemble," "Computational," and "Nominal." While a comprehensive discussion of the taxonomy is outside the scope of this essay, our review of the empirical clustering of articles into the five categories indicates that little if any IT research has examined characteristics of IT artifacts related to user security, privacy, protection from harm, and other attributes associated with user security controls.

Attention to the nature of the security control artifact is important in determining whether current theoretical models explain technology use (or non-use) and user adoption of security controls. One must first examine the factors defining a general IT artifact for which models such as TAM and UTAUT were developed, and then compare those with factors defining security control artifacts such as firewalls and antivirus software.

To provide a theoretical framework for this comparison, we employ Herzberg's two-factor Theory of Motivation (Herzberg 1966, 1968, 1987), not to argue its validity as a motivational theory in its original context, but to use it as a theoretical framework for differentiating IT artifacts. Herzberg's theory is based on his observation that some job factors seem to be predictors of job satisfaction, while others predict job dissatisfaction. He termed the predictors of job satisfaction *motivators*, and the predictors of job dissatisfaction *hygiene factors*. Herzberg further defined motivators as factors that tended to be under the control of an individual and motivated them through their intrinsic need for achievement, recognition, etc. On the other hand, hygiene factors provide a necessary, but not sufficient condition for worker satisfaction. Hygiene factors include features such as company policy, relationships with peers and supervisors, salary, and security (Herzberg, 1987).

Recently, Zhang and von Dran (2000) used the two-factor model to evaluate and characterize Website design factors. They note that while Herzberg's methodology has been criticized, it also has been used extensively in job redesign projects, the success of which is documented in several studies (Kopelman, 1986). They also note that Herzberg's theory has been successfully used as a management tool in many other areas, and argue that the two-factor model has the following useful aspects:

> "First, the dual structure, that is, the distinction between satisfaction and dissatisfaction as two dimensions rather than two values of the same dimension is logical and valuable. Not being dissatisfied does not mean being satisfied. Not being satisfied does not mean one is dissatisfied. Second, the concept of hygiene is appropriate once one understands its meaning as being preventive and environmental in nature. Third, relating factors to perceived satisfaction and dissatisfaction is a way of examining the factors in the Website environment." (p. 1256).

Use of the two-factor framework continues today in a wide variety of contexts. To investigate customer satisfaction, for example, Turner and Krizek (2006) note that it "offers a way to focus on relationships between experiences, a vocabulary for discussing those relationships, and a multidimensional model of satisfaction" (p. 126) and dismiss concerns about generalizability as irrelevant due to the impossibility of a single universal taxonomy.

Inferring Characteristics of IT Artifacts in Existing Models

While few studies provide a detailed description of the characteristics of the IT artifact under study, we can attempt to make inferences by examining the definitions of the constructs used in the models and by examining the instruments used in the studies. For example, the Davis (1989) study that describes TAM specifically addresses the electronic mail artifact. One of the core constructs of TAM is *perceived usefulness*, the extent to which people believe technology will help them perform their job. Viewing the *perceived usefulness* definition within the framework provided by Herzberg's two-factor model, it seems reasonable to assume that Davis is targeting IT artifacts rich in *motivating* factors. Further support for this assumption can be found by studying the survey questions presented in table 2. The questions appear to measure artifacts for which the user perceives a positive relationship between use and expected rewards for doing their job well.

Table 2. Questions Measuring Perceived Usefulness (Davis, 1989)

1.	Using the system in my job would enable me to accomplish tasks more quickly.
2.	Using the system would improve my job performance.
3.	Using the system in my job would increase my productivity.
4.	Using the system would enhance my effectiveness on the job.
5.	Using the system would make it easier to do my job.
6.	I would find the system useful in my job.

In developing the UTAUT model, Venkatesh, et al., (2003) defined a construct called *performance expectancy* as "the degree to which an individual believes that using the system will help him or her attain gains in job performance" (p. 447). They found that the performance expectancy construct proved to be the strongest predictor of intention within each of the eight models studied, and that it remained significant at all points of measurement in both voluntary and mandatory settings. Analogous to TAM, UTAUT's performance expectancy seems to address IT artifacts rich in motivating factors. Examining the survey questions used to measure performance expectancy provides additional support for this assumption (see table 3).

Table 3. Questions Measuring Performance Expectancy (Venkatesh, et al., 2003)

1. I would find the system useful in my job.
2. Using the system enables me to accomplish tasks more quickly.
3. Using the system increases my productivity.
4. If I use the system, I will increase my chances of getting a raise.

The other two constructs that Venkatesh et al. (2003) found to directly influence intention to use were *effort expectancy* (how easy it is to use an IT artifact) and *social influence* (whether important peers and supervisors believe the IT artifact should be used). The definition of effort expectancy would seem to indicate that it is a hygiene factor, impacting a user's dissatisfaction with an IT artifact, but not their satisfaction. The definition of s*ocial influence* and the questions used by Venkatesh et al. (2003) would seem to fit Herzberg's (1987) classification as a hygiene factor. However, it may also be the case that using a system will increase an individual's recognition, meaning that social influence may also display characteristics of a motivator, increasing ones satisfaction with a system. They also found a significant relationship between usage behavior and facilitating conditions. *Facilitating conditions* is defined as "the degree to which an individual believes that an organizational and technical infrastructure exists to support use of the system" (p. 453). Similar to effort expectancy, the definition of facilitating conditions seems to suggest that it may be a hygiene factor and impacts system dissatisfaction.

Regardless of how effort expectancy, social influence, and facilitating conditions are classified using the criteria described in the two-factor model, it seems clear that these are constructs that can be used to examine the acceptance of any IT artifact. This is not the case with performance expectancy as it is defined in the current user acceptance theories. Performance expectancy is defined only in terms of motivators, and not all IT artifacts have a direct impact on job performance. Security control systems (e.g. firewalls, virus protection software, anti-spyware software, etc.) would be an example of this. These IT artifacts mitigate threats against a computer system, providing security against attacks on the system. According to Herzberg's model, security is considered a hygiene factor and, as such, impacts dissatisfaction with a system, not satisfaction. In other words, the current theoretical models concerning technology acceptance assume, either explicitly or implicitly, that using a specific technology will result in no harm and could, potentially, result in some benefits (e.g., job performance improvement). If a user chooses not to use a system, the non-use results in no harm or benefit.

This assumption does not hold for security controls. Instead, non-use of security controls will possibly result in harm (e.g. the computer system is compromised) and no benefit. Conversely, the use of security control systems may reduce the risk that harm will occur, without supplying tangible benefits to the user. For example, not implementing a firewall will increase the probability that a user's computer system will be compromised by an external attacker. Implementing the firewall will mitigate the risk of external attack, but will provide no direct benefit to the user in terms of improving the user's job performance.

Moving Toward a Model for a Security Control Artifact

The above discussion calls into question how well current technology acceptance models accurately predict user acceptance of security controls. As noted above, performance expectancy is one of the strongest predictors of intention to use and is a fundamental construct of all the prominent technology acceptance models. However, it seems unlikely that users perceive the use of security controls as providing any tangible benefits in terms of improved job performance. Therefore, we suggest that the performance expectancy construct, as defined in UTAUT and other theories of technology acceptance, will have little predictive power when applied to security control technologies. Obviously, additional research is needed to empirically support or refute this claim. If future studies show that theories such as UTAUT are inappropriate for predicting security control usage, then additional theory development specifically for security control artifacts will be necessary.

One research area that may prove helpful in developing the necessary theories is the study of the cognitive processes involved in protection behavior. An example of a theory from this area that may be applicable to security control artifacts is Rogers' Protection Motivation Theory (PMT). PMT was first proposed by Rogers in 1975 to predict an individual's cognitive reaction to a fear appeal. A *fear appeal* can be defined as a message informing an individual that (1) a specific threat is acute; (2) the threat places an individual at risk; (3) there are recommended behaviors that allay the risk; and (4) an individual should adopt the recommended behaviors (Rogers 1975, 1983). As noted by Rogers, fear appeals are ubiquitous and used in many areas to attempt to modify behavior, including attempts to motivate users to adopt security controls. Rogers revised PMT in 1983 into a more general theory, adding additional information sources such as observational learning, personality, and prior experience. Rogers also added *self-efficacy* to the *coping appraisal* process, acknowledging the importance of social learning theory (Rogers 1983; Milne et al. 2000; Bandura 1977).

PMT has been used extensively to study issues concerning areas such as health care, public safety, and the environment. In general, PMT proposes that an individual's motivation to adopt a behavior recommended by a fear appeal is a function of the individual's cognitive appraisals of the threat and the recommended coping response. PMT additionally proposes that the threat appraisal is a linear function of the intrinsic and extrinsic value an individual places on a noxious behavior (e.g. the internal addictive characteristic of cigarette smoking), the perceived severity of the proposed threat, and an individual's perceived vulnerability to the threat. Similarly, the coping appraisal is a linear function of the recommended behavior's response efficacy (will it work?), the individual's self-efficacy (can I do it?), and any costs associated with the recommended behavior. Figure 3 shows a modern adaptation of PMT. Note that PMT acknowledges and predicts maladaptive coping responses such as avoidance, and denial.

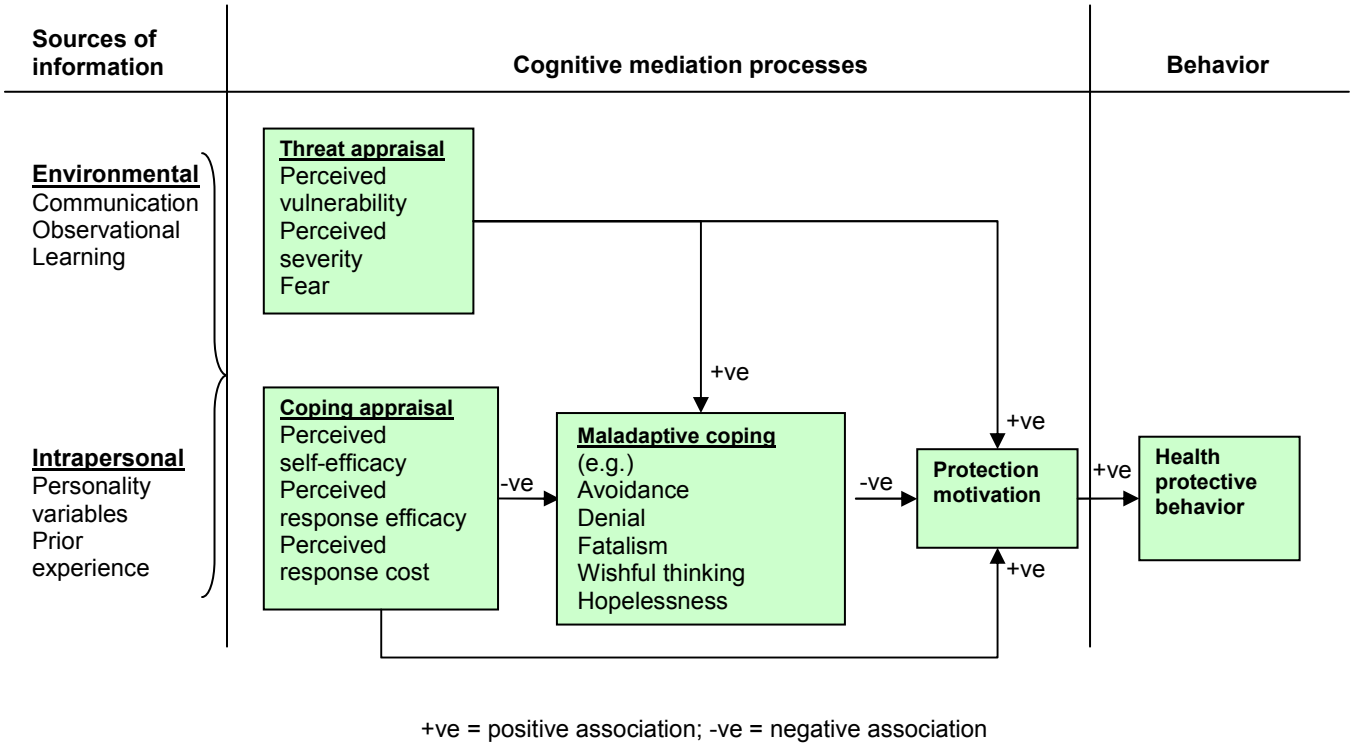

Figure 3. Protection Motivation Theory (from Milne et al., 2000)

PMT Work in Security Control Adoption Research

To date, one of the few instances of PMT used to study security control adoption is Woon et al. (2005). Their work centered on identifying predictors that differentiate between wireless home network users who implement security controls from those who don't. Woon et al. did not focus on specific security controls (e.g. firewalls, virus protection software, etc.), and left it up to each individual to interpret what was meant by *enable security features*. They did, however, include a measure of the knowledge each respondent had concerning general network security. Woon et al. found that while *perceived vulnerability* was not significant in determining a respondent's intention to enable security measures, the relationships between *perceived severity*, *response efficacy*, *self-efficacy*, and *response cost* and *intention* to enable security measures were all significant.

To identify commonalities and differences, the following section examines Woon et al.'s adaptation of PMT to the security control adoption problem and compares their adaptation to the UTAUT model. Of significant interest at the outset it that UTAUT has no constructs that correspond to PMT's *perceived vulnerability* and *perceived severity*. Woon et al. (2005) defined *perceived vulnerability* as a user's assessment of his/her own probability of being exposed to unauthorized access to the user's wireless network. They defined *perceived severity* as a measure of the perceived magnitude of what might happen if the threat succeeds. The consequences were presented to the respondents as the potential loss of personal information and online identity (Woon, et al., 2005).

UTAUT likely does not include these constructs because it focuses on IT artifacts where there is a tangible benefit from use, not on artifacts that represent only intangible benefit from use and potential harm from non-use. Given the characterization of security control artifacts it seems logical that any theory attempting to explain their adoption will require constructs such as perceived vulnerability and perceived severity, which attempt to measure the influence of this potential harm. This is another area where additional research is needed to empirically support or refute this claim.

Conversely, PMT does not include constructs that measure *social influence* and *facilitating conditions*, as it was designed to explain the internal cognitive processes one undergoes when evaluating a threat and potential behavioral responses. Given that a significant body of technology adoption literature supports a relationship between both social influence and facilitating conditions (as defined in UTAUT) and the adoption of technology, it seems reasonable to assume that such a relationship may exist for security control adoption. This is another area where additional empirical research is necessary.

UTAUT defines the *effort expectancy* construct as "the degree of ease associated with the use of the system" (Venkatesh, et al., 2003, p. 450). PMT's *response costs* construct is similar but more general. Woon et al. (2005) defined response costs as the perceived costs incurred by a user in performing a recommended coping behavior (i.e., enabling network security) and included items such as economic cost, difficulty, inconvenience, and related side effects. This difference is further highlighted in the survey questions used by Venkatesh et al. (2005) to measure effort expectancy (table 4) and those used by Woon et al. to measure response cost (table 5).

Table 4. Questions Measuring Effort Expectancy (Venkatesh, et al, 2003)

1. My interaction with the system would be clear and understandable.
2. It would be easy for me to become skillful at using the system.
3. I would find the system easy to use.
4. Learning to operate the system is easy for me.

Table 5. Questions Measuring Response Cost (Woon, et al., 2005)

1. The cost of enabling security measures decreases the convenience afforded by a home wireless network.
2. There are too many overheads associated with trying to enable security measures on a home wireless network.
3. Enabling security features on my wireless router would require considerable investment of effort other than time.
4. Enabling security features on a wireless router would be time consuming.

Woon et al.'s definition of response cost is intuitively appealing, as it is reasonable that the costs incurred implementing a security control encompass more than just the effort involved in the adoption. However, this is another area were additional research is needed to empirically validate the inclusion (or exclusion) of UTAUT's effort expectancy construct and PMT's response cost construct.

Both PMT and UTAUT include similar definitions of self-efficacy. Woon et al. (2005) defined self-efficacy as how well the respondent could perform the recommended coping behavior (referring to security features). Similarly, self-efficacy was defined by Venkatesh et al. as one's perceived ability to use a technology to accomplish a task. The similarities are further highlighted in the survey questions used by Venkatesh et al. (table 6) and Woon et al. (table 7) to measure self-efficacy.

Table 6. Questions Measuring Self-efficacy (Venkatesh, et al., 2003)

I could complete a job or task using the system…
1. If there was no one around to tell me what to do as I go.
2. If I could call someone for help if I got stuck.
3. If I had a lot of time to complete the job for which the software was provided.
4. If I had just the built-in help facility for assistance.

Table 7. Questions Measuring Self-efficacy (Woon, et al., 2005)

1. It would be easy for me to enable security features on the home wireless network by myself.
2. I could enable wireless security measures if there was no one around to tell me what to do as I go along.

One of the many interesting results of UTAUT, however, is that when controlling for effort expectancy, self-efficacy did **not** have a significant influence on behavioral intention to adopt, and therefore was not included in the final model. This contradicts PMT, where studies using PMT consistently find that the association between self-efficacy and behavioral intention is the strongest of any of the PMT constructs (Milne et al. 2000). This curious conflict is another area where additional empirical research is needed.

Finally, both UTAUT and PMT include a conceptualization of the expected performance of the targeted IT artifact. However, the manner in which these conceptualizations are defined and operationalized is quite different. In UTAUT, the concept is incorporated into the *performance expectancy* construct which, as noted above, is defined as how well the individual believes that using the system will help him or her to improve job performance. Note the focus of this definition on perceived benefits from using the system. PMT incorporates this concept into its *response efficacy* construct. Woon et al. (2005) define response efficacy as the belief that the recommended response (i.e., enabling wireless security features) will be effective in reducing the risk of unauthorized access to a user's wireless network. The difference, then, between UTAUT's performance expectancy construct and PMT's response efficacy construct is that performance expectancy is defined in terms of system benefits (motivator factors) while response efficacy is defined in terms of threat mitigation (hygiene factors). This is further highlighted by comparing the survey questions displayed in table 3 with the Woon et al. (2005) questions in table 8.

Table 8. Questions Measuring Response Efficacy (Woon, et al., 2005)

1. Enabling security measures on my home wireless network will prevent hackers from stealing network bandwidth.
2. Enabling the security measures on a home wireless network is an effective way of deterring hacker attacks.
3. Enabling security measures on my home wireless network will prevent hackers from gaining important personal or financial information.
4. Enabling security measures on my home wireless network will prevent hackers from stealing my identity.

To emphasize one of the most important distinctions between the UTAUT and PMT approaches to technology acceptance, it may be difficult for UTAUT to detect perceived benefits from adopting security controls because users will not perceive that using security controls will increase job performance. Instead, the benefits of adopting security controls must be viewed in terms of their mitigating effect on the risks posed by external entities gaining access to a user's computer system, which is considered a hygiene factor and detectable in the PMT approach. Thus it is reasonable to expect that PMT's response efficacy construct is more appropriate for security control adoption than UTAUT's performance expectancy construct. As mentioned before, additional research is needed to empirically confirm or refute this claim.

Conclusion

Most existing research in technology acceptance ignores important aspects of the IT artifact. In the context of security control adoption by users, this is a significant shortcoming because the motivation for using security controls is related to mitigating negative threats rather than achieving positive benefits. This critical essay examines prior research, primarily UTAUT and PMT, and represents a small but important step toward the development of a theory for the adoption of security controls. In employing a two-factor approach to investigate both hygiene factors that may incorporate threat and risk, and motivators that include potential benefit, we believe a more powerful explanatory framework is possible.

Our work shows that, while UTAUT and PMT contain constructs that are nearly identical, they each also contain unique elements not found in the other. This argues for additional empirical research that focuses on a unified model for security control adoption, possibly containing elements from both the current technology adoption literature and theories, such as PMT, which focuses on areas such as protection behavior. In particular, we recommend additional research that focuses on:

- Empirically validating the appropriateness of existing technology acceptance models, such as UTAUT, for predicting security control usage. In particular, assessing and possibly redefining the *performance expectancy* construct so that it better fits the security control artifact.
- Empirically measuring the usefulness of constructs such as *perceived vulnerability*, *perceived severity*, and *response costs*, as defined by PMT, as determinants of security control adoption.
- Empirically measuring the usefulness of constructs such as *social influence* and *facilitating conditions*, as defined by UTAUT, as determinants of security control adoption.
- Empirically measuring the importance of *self-efficacy*, as defined in both UTAUT and PMT, to the adoption of security controls.

Following additional theory and model development, we intend to test reformulations of UTAUT and PMT in the context of security control adoption. The ultimate goal is to identify a robust yet parsimonious model having explanatory and predictive power covering a wider range of IT artifact types than has traditionally been possible.

References

Ajzen, I. "The Theory of Planned Behavior." *Organizational Behavior and Human Decision Processes* (50:2), 1991, pp. 227-47.

Bandura, A. "Self-Efficacy: Toward a Unifying Theory of Behavioral Change." *Psychological Review* (84), 1977, pp. 191-215.

Davis, F. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly* (13:3), 1989, pp. 319-340.

Davis, F., Bagozzi, R., Warshaw, P. "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models." *Management Science* (35:8), 1989, pp. 982-1003.

Fishbein, M. and Ajzen, I. *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*, Addison-Wesley, Reading, MA, 1975.

Herzberg, F. *Work and the Nature of Man*. New York, New World Publishing, 1966.

Herzberg, F. "One More Time: How Do You Motivate Employees?" *Harvard Business Review*, Jan/Feb 1968, pp. 53-62.

Herzberg, F. "One More Time: How Do You Motivate Employees?" *Harvard Business Review*, Sep/Oct 1987, pp. 109-120.

Karahanna, E. and Straub, D. "Information Technology Adoption across Time: A Cross-Sectional Comparison of Pre-Adoption and Post-Adoption Beliefs," *MIS Quarterly* (23:2), 1999, pp. 183-213.

Kopelman, R. *Managing Productivity in Organizations*. New York: McGraw-Hill, 1986.

Milne, S., Sheeran, P., and Orbell, S. "Prediction and Intervention in Health-Related Behavior: A Meta-Analytic Review of Protection Motivation Theory." *Journal of Applied Social Psychology* (30:1), 2000, pp. 106-143.

NIST (US National Institute of Standards and Technology). "Wireless Network Security" 2002. Available from http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf

Orlikowski, W. and Iacono, C. "Research Commentary: Desperately Seeking the 'IT' in IT Research – A Call to Theorizing the IT Artifact." *Information Systems Research* (12:2), 2001, pp. 121-134.

PANDA Software International, "Security in Wireless Networks," accessed June 15, 2006 at http://vocuspr.vocus.com/VocusPR30/Temp/Sites/2631/28d2f2c9bfeb4c808531a849e150d810/WP%20Wifi.pdf

Potter, B. "Wireless Hotspots: Petri Dish of Wireless Security." *Communications of the ACM* (49: 6), 2006, pp. 51-56.

Rogers, R. "A Protection Motivation Theory of Fear Appeals and Attitude Change." *The Journal of Psychology* (91), 1975, pp. 93-114.

Rogers, R. "Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation." In B.L.Cacioppo & L.L. Petty (eds.), *Social Psychophysiology: A Sourcebook*, Guilford, London, U.K. (1983), pp. 153-176.

Turner, P. and Krizek, R. "A Meaning-Centered Approach to Customer Satisfaction." *Management Communication Quarterly* (20:15), 2006, pp. 115-147.

Venkatesh, V., Morris, M., Davis, G., and Davis, F. "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly* (27:3), 2003, pp. 425-478.

Woon, I.M.Y. Tan, G.W., and Low, R.T. "A Protection Motivation Theory Approach to Home Wireless Security." *Proceedings of the Twenty-Sixth International Conference on Information Systems*, Las Vegas, NV, 2005, pp. 367-80.

Zhang, P. and von Dram, G. "Satisfiers and Dissatisfiers: A Two-Factor Model for Website Design and Evaluation." *Journal of the American Society for Information Science* (51:14), 2000, pp. 1253-1268.